



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/787,361	02/27/2004	Hironobu Machida	036741-0130	7946

22428 7590 05/09/2008  
FOLEY AND LARDNER LLP  
SUITE 500  
3000 K STREET NW  
WASHINGTON, DC 20007

EXAMINER

RILEY, MARCUS T

ART UNIT

PAPER NUMBER

2625

MAIL DATE

DELIVERY MODE

05/09/2008

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

### Office Action Summary

**Application No.**

10/787,361

**Applicant(s)**

MACHIDA ET AL.

**Examiner**

MARCUS T. RILEY

**Art Unit**

2625

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 16 January 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-19 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-19 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 27 February 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-8508)  
Paper No(s)/Mail Date 02/27/2004, 12/18/2007
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Inventor's Patent Application
- 6) ☐ Other: \_\_\_\_\_

## DETAILED ACTION

### Response to Amendment

1. This office action is responsive to applicant's remarks received on January 16, 2008. Claims 1-19 remain pending.

### Response to Arguments

2. Applicant's arguments with respect to amended **claims 1, 2, 6, 7-13, 18 & 19** filed on January 16, 2008 have been fully considered but they are not persuasive.

### A: Applicant's Remarks

*In the Office Action, claims 1-3 were rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,850,716 to Kurihara; claims 4 and 5 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Kurihara in view of U.S. Patent No. 5,606,613; claims 6-11 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Kurihara in view of Lee and further in view of U.S. Patent No. 5,903,647 to Ronning; claims 12 and 18 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,058,476 to Matsuzaki et al. in view of Ronning; claims 13-19 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Matsuzaki et al. in view of Ronning and further in view of U.S. Patent No. 6,023,506 to Ote et al.; claim 14 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Matsuzaki et al., Ronning and Ote et al. and further in view of U.S. Patent No. 7,124,094 to Kobayashi et al.; claim 15 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Matsuzaki et al. and Ronning and further in view of U.S. Patent No. 7,024,500 to Ashizaki et al.; claim 16 was rejected under 35 U.S.C. § 103(a) as being unpatentable over*

*Matsuzaki et al., Ronning and Ote et al. and further in view of Ashizaki et al; and claim 17 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Matsuzaki et al., Ronning, Ote et al. and Kobayashi, and further in view of Ashizaki et al. These rejections are traversed with respect to the presently pending claims under rejection, for at least the reasons given below.*

*The present invention is directed to preventing internal information of a Hard Disk Drive (HDD) of a copying apparatus from being decoded after the HDD is removed from the copying apparatus. As such, the present invention has a feature of including an encryption key memory for storing an encryption key used for encryption and decryption.*

*The encryption key memory (see memory 820 in Figure 1 of the drawings, for example) is a volatile memory, and corresponds to the volatile storage means recited in claim 1. The encryption key is set when power is switched on and the encryption key is erased when power is switched off. Accordingly, the present invention can prevent the internal information stored in an HDD from being decoded even when the HDD is stolen at the time of power off, since the encryption key has been erased.*

*By contrast, Kurihara describes a non-volatile environment configuring memory 11. However, the environment configuring memory 11 is not used for storing an encryption key. That is, Kurihara fails to disclose or suggest a encryption key that is stored in a non-volatile memory.*

*Accordingly, presently pending independent claim 1 is not anticipated by Kurihara.*

*With respect to presently pending independent claims 12 and 18, those claims now recite a display means for prompting a user to input a key a plurality of times.*

*Neither Matsuzaki et al. nor Ronning teaches or suggests such a display means as recited in claims 12 and 18. In particular, while Figure 9 of Matsuzaki shows an encryption apparatus*

*that has a monitor, there is no teaching or suggestion that this monitor prompts a user to input a key a plurality of times. Ronning is used in the Office Action to show a non-volatile memory, and fails to rectify the above-mentioned deficiencies of Matsuzaki.*

*Thus, presently pending independent claims 12 and 18 are patentable over the cited art of record.*

*Since all of the issues raised in the Office Action have been addressed in this Amendment and Reply, Applicants believe that the present application is now in condition for allowance, and an early indication of allowance is respectfully requested.*

**A: Examiner's Response**

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Thus, the previous claim rejection under 35 USC §102 is withdrawn in light of the applicant's amendments. **Claims 1-3** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kurihara (US 6,850,716 B2 hereinafter, Kurihara '716) in combination with Bright et al. (US 4,262,329 hereinafter, Bright '329). **Claims 4** is rejected under 35 U.S.C. 103(a) as being unpatentable over Kurihara '716 in combination with Lee et al. (US 5,606,613 hereinafter, Lee '613). **Claim 5** is rejected under 35 U.S.C. 103(a) as being unpatentable over Kurihara '716 and Bright '329 as applied to claim 1, and further in view of Lee '613. **Claims 6-11** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kurihara '716, Bright '329 and Lee '613 as applied to claim 1, and further in view of Ronning (US 5,903,647 hereinafter, Ronning '647). **Claims 12, 13, 18 & 19** are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsuzaki et al. (US 6,058,476 hereinafter, Matsuzaki '476) in combination with Ronning '647 as applied to claim 1, and further in view of Ote et al. (US 6,023,506 hereinafter, Ote '506).

**Claim 14** is rejected under 35 U.S.C. 103(a) as being unpatentable over Matsuzaki '476, Ronning '647 and Ote '506 as applied to claim 12, and further in view of Kobayashi et al. (US 7,124,094 hereinafter, Kobayashi '094). **Claims 15 & 16** are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsuzaki '476, Ronning '647 and Ote '506 as applied to claim 12, and further in view of Ashizaki et al. (US 7,024,500 hereinafter, Ashizaki '500). **Claim 17** is rejected under 35 U.S.C. 103(a) as being unpatentable over Matsuzaki '476, Ronning '647, Ote '506 and Kobayashi '094 as applied to claim 12, and further in view of Ashizaki '500. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Kurihara '716 in combination with Bright '329 discloses encryption and decryption means that encrypts image data using an encryption key prior to the storage of the input image data onto image storage means, and decrypts the encrypted image data subsequent to the reading of the encrypted image data from the image storage means (*"Further, it is also possible to encrypt and store the program of the present invention on a storage medium such as a CD-ROM, distribute the storage medium to users, allow users who meet certain requirements to download decryption key information from, e.g., a website via the Internet, and allow these users to run the encrypted program by using the key information, whereby the program is installed in the user computer."* column 10, lines 33-39).

Kurihara '716 does not expressly disclose a volatile storage means that stores an encryption key to be set when power is on. However, Bright '329 discloses a volatile storage means that stores an encryption key to be set when power is on (*"The CPU 38 performs most of the work of the Hard-Node. It does the encryption and decryption, authorization checks,*

*communications with the host machine 32, and directs the activities of the data channels 54. The CPU 38 operates under control of a program, stored in Program Storage 56. This is one of the several sections of storage addressable by the CPU, the others being Scratchpad Storage 58 and the Superkey Register 60. Scratchpad Storage 58 is used for buffers, intermediate encryption results and other temporary data. The Superkey Register holds the Hard-Node's own Superkey under which the Key Data Base, at least, is encrypted. For maximum security, it is recommended that the Superkey Register 60 be a volatile storage device with its own battery and interlock to remove all power in case the enclosure 42 is tampered with or opened. The Scratchpad Storage 58 should be a volatile random access memory device, while the Program Storage 56 should be a nonvolatile ROM (read only memory) device."* column 3, lines 12-31). See also ("*At log-on time, it sends an encrypted password to identify the user to the central site Hard-Node, which looks it up in its Key Data Base. The user's key is entered into the micro-Hard-Node's volatile Key Register (analogous to the Hard-Node's Superkey Register) via a Key Entry device, which may be a magnetic stripe reader.*" column 5, lines 19-26). Thus, Kurihara '716 in combination with Bright '329 discloses the elements of claim 1. Accordingly, claim 1 is rejected by the combination of Kurihara '716 and Bright '329.

With respect to presently pending independent claims 12 and 18 and in accordance with Applicant's amendment, claims 12 and 18 now recite a display means for prompting a user to input a key a plurality of times. Matsuzaki '476 in combination with Ronning '647 and further in view of Ote '506 discloses displaying an image on a screen so as to prompt a user to input a key a plurality of times when power is on ("*Upon starting the file encryption/decryption means 1000 to conduct decryption, the file encryption/decryption means 1000 conducts authentication*

*processing by using the password 1070 with respect to a user input password, then refers to the unencrypted file /encrypted file association table 1060, and displays a list of encrypted files 1090 stored in the encrypted file area 1080 in the form of unencrypted file names. In this state, the encryption folder 1040 is open. The user can select unencrypted files 1090 stored in the encrypted file area 1080 out of the list displayed in the form of unencrypted file names.”* column 5, lines 5-15). Thus, presently pending independent claims 12 and 18 are not patentable over the cited art of record.

Accordingly, claims 1-19 remain pending and amended **claims 1, 2, 6, 7-13, 18 & 19** have been fully considered but they are not persuasive. As a result, the present application is not in condition for allowance.

#### **Claim Objections**

***(The previous claim objections are withdrawn in light of the applicant's amendments.)***

#### **Claim Rejections - 35 USC § 103**

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. **Claims 1-3** are rejected under 35 U.S.C. 103(a) as being unpatentable Kurihara '716 in combination with Bright '329.



**Regarding claim 1;** Kurihara '716 discloses an image forming apparatus for forming an image based on input image data, the image forming apparatus comprising: encryption and decryption means that encrypts image data using an encryption key prior to the storage of the input image data onto image storage means, and decrypts the encrypted image data subsequent to the reading of the encrypted image data from the image storage means (*"Further, it is also possible to encrypt and store the program of the present invention on a storage medium such as a CD-ROM, distribute the storage medium to users, allow users who meet certain requirements to download decryption key information from, e.g., a website via the Internet, and allow these users to run the encrypted program by using the key information, whereby the program is installed in the user computer."* column 10, lines 33-39).

Kurihara '716 does not expressly disclose a volatile storage means that stores an encryption key to be set when power is on.

Bright '329 discloses a volatile storage means that stores an encryption key to be set when power is on (*"The CPU 38 performs most of the work of the Hard-Node. It does the encryption and decryption, authorization checks, communications with the host machine 32, and directs the activities of the data channels 54. The CPU 38 operates under control of a program, stored in Program Storage 56. This is one of the several sections of storage addressable by the CPU, the others being Scratchpad Storage 58 and the Superkey Register 60. Scratchpad Storage 58 is used for buffers, intermediate encryption results and other temporary data. The Superkey Register holds the Hard-Node's own Superkey under which the Key Data Base, at least, is encrypted. For maximum security, it is recommended that the Superkey Register 60 be a volatile storage device with its own battery and interlock to remove all power in case the enclosure 42 is*

*tampered with or opened. The Scratchpad Storage 58 should be a volatile random access memory device, while the Program Storage 56 should be a nonvolatile ROM (read only memory) device.” column 3, lines 12-31). See also (“At log-on time, it sends an encrypted password to identify the user to the central site Hard-Node, which looks it up in its Key Data Base. The user's key is entered into the micro-Hard-Node's volatile Key Register (analogous to the Hard-Node's Superkey Register) via a Key Entry device, which may be a magnetic stripe reader.” column 5, lines 19-26); and*

Kurihara '716 and Bright '329 are combinable because they are from same field of endeavor of data processing systems (*“It is an object of this invention to provide a new and improved data processing security system.”* Bright '329 at column 3, lines 15-16).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the data processing system as taught by Kurihara '716 by adding a volatile storage means that stores an encryption key to be set when power is on as taught by Bright '329.

The motivation for doing so would have been because it is advantageous to provide to provide a new and improved security system for data processing installations which is especially suitable for commercial use (*“Another object is to provide a new and improved security system for data processing installations which is especially suitable for commercial use.”* Bright '329 at column 1, lines 47-49).

Therefore, it would have been obvious to combine Kurihara '716 with Bright '329 to obtain the invention as specified in claim 1.

**Regarding claim 2;** Kurihara '716 discloses a non-volatile storage means for storing the encryption key, wherein the encryption and decryption means temporarily stores the encryption

key, sent from the non-volatile storage means, in a temporary storage unit there within when the image data is stored onto the image storage means or when the encrypted image data is read from the image storage means (*"An environment configuring memory 11 comprising a non-volatile read/write memory (referred to as an "NVRAM" below) saves various operating environment settings of the image forming apparatus 30. column 2, lines 27-30).* See also (*"Further, it is also possible to encrypt and store the program of the present invention on a storage medium such as a CD-ROM, distribute the storage medium to users, allow users who meet certain requirements to download decryption key information from, e.g., a website via the Internet, and allow these users to run the encrypted program by using the key information, whereby the program is installed in the user computer."* column 10, lines 33-39).

**Regarding claim 3;** Kurihara '716 discloses where the encryption and decryption means and the non-volatile storage means are arranged in separate units (*"Further, it is also possible to encrypt and store the program of the present invention on a storage medium such as a CD-ROM, distribute the storage medium to users, allow users who meet certain requirements to download decryption key information from, e.g., a website via the Internet, and allow these users to run the encrypted program by using the key information, whereby the program is installed in the user computer."* column 10, lines 33-39).

5. **Claims 4** is rejected under 35 U.S.C. 103(a) as being unpatentable over Kurihara '716 in combination with Lee '613.

**Regarding claim 4;** Kurihara '716 discloses an image forming apparatus for forming an image based on input image data, the image forming apparatus comprising encryption and decryption means that encrypts image data using an encryption key prior to the storage of the input image data onto image storage means, and decrypts the encrypted image data subsequent to the reading of the encrypted image data from the image storage means (*"Further, it is also possible to encrypt and store the program of the present invention on a storage medium such as a CD-ROM, distribute the storage medium to users, allow users who meet certain requirements to download decryption key information from, e.g., a website via the Internet, and allow these users to run the encrypted program by using the key information, whereby the program is installed in the user computer."* column 10, lines 33-39).

Kurihara '716 does not expressly disclose an encryption key generating means for generating a random number and producing the encryption key that contains at least a portion of the generated random number.

Lee '613 discloses an encryption key generating means for generating a random number and producing the encryption key that contains at least a portion of the generated random number (*"In operation, upon power-up of the system or at such other selected times, the verification circuit in response to a power-up print command (Print Cmmd) from the meter 10 outputs a random number message to the decryption/encryption engine 37 which encrypts the message in response to the power-up print command. The encrypted message is sent out to the meter. The encryption/decryption engine 37 of the vault decrypts the message in response to the print command."* column 3, lines 61-67 thru column 4, lines 1-2).

Kurihara '716 and Lee '613 are combinable because they are from same field of endeavor of an image forming apparatus (*"The present invention relates to a postage metering system using digital printing..."* Lee '613 at column 1, lines 6-7).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the image forming apparatus as taught by Kurihara '716 by adding an encryption key generating means for generating a random number and producing the encryption key that contains at least a portion of the generated random number as taught by Lee '613.

The motivation for doing so would have been in order to assure full and accurate accounting of the printer (*"In order to assure full and accurate accounting for the particular digital printer, upon power-up of the system or at such other pre-selected condition, the print controller module of the digital printer sends out an encrypted message to the meter."* Lee '613 at column 2, lines 14-19).

Therefore, it would have been obvious to combine Kurihara '716 with Lee '613 to obtain the invention as specified in claim 1.

6. **Claim 5** is rejected under 35 U.S.C. 103(a) as being unpatentable over Kurihara '716 and Bright '329 as applied to claim 1 above, and further in view of Lee '613.

**Regarding claim 5;** Kurihara '716 and Bright '329 does not expressly disclose an encryption key generating means for generating a random number and producing the encryption key that contains at least a portion of the generated random number.

Lee '613 discloses encryption key generating means for generating a random number and producing the encryption key that contains at least a portion of the generated random number

*("In operation, upon power-up of the system or at such other selected times, the verification circuit in response to a power-up print command (Print Cmmnd) from the meter 10 outputs a random number message to the decryption/encryption engine 37 which encrypts the message in response to the power-up print command. The encrypted message is sent out to the meter. The encryption/decryption engine 37 of the vault decrypts the message in response to the print command."* column 3, lines 61-67 thru column 4, lines 1-2).

Kurihara '716 and Bright '329 are combinable with Lee '613 because they are from same field of endeavor of an image forming apparatus (*"The present invention relates to a postage metering system using digital printing..."* Lee '613 at column 1, lines 6-7).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the image forming apparatus as taught by Kurihara '716 and Bright '329 by adding an encryption key generating means for generating a random number and producing the encryption key that contains at least a portion of the generated random number as taught by Lee '613.

The motivation for doing so would have been in order to assure full and accurate accounting of the printer (*"In order to assure full and accurate accounting for the particular digital printer, upon power-up of the system or at such other pre-selected condition, the print controller module of the digital printer sends out an encrypted message to the meter."* Lee '613 at column 2, lines 14-19).

Therefore, it would have been obvious to combine Kurihara '716 and Bright '329 with Lee '613 to obtain the invention as specified in claim 1.

7. **Claims 6-11** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kurihara '716, Bright '329 and Lee '613 as applied to claim 1 above, and further in view of Ronning '647.

**Regarding claim 6;** Kurihara '716, Bright '329 and Lee '613 does not expressly disclose an encryption key compression and decompression means for compressing or decompressing the encryption key using a predetermined compression and decompression method, wherein the compressed encryption key is stored onto the non-volatile storage means and when the encryption key is used, the compressed encryption key is read from the non-volatile storage means.

Ronning '647 discloses an encryption key compression and decompression means for comprsing or decompressing the encryption key using a predetermined compression and decompression method, wherein the compressed encryption key is stored onto the non-volatile storage means and when the encryption key is used, the compressed encryption key is read from the non-volatile storage means (*"The system decrypts the sectors while reading them. The encryption/decryption of sector is explained with reference to FIGS. 16A and 16B. If the sectors of the application are compressed the system also decompresses the sectors while reading them."* column 8, lines 21-25). See also (*"An image file 77 which is the desired size of a "virtual volume" created by a software or digital information distribution system is allocated on a hard drive 75 or other non-volatile storage medium."* column 6, lines 14-18).

Kurihara '716, Bright '329 and Lee '613 are combinable with Ronning '647 because they are from same field of endeavor of an image forming apparatus (*"The system typically uses an image driver 56..."* Ronning '647 at column 5, lines 19-20).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the image forming apparatus as taught by Kurihara '716, Bright '329 and Lee '613 by adding an encryption key compression and decompression means for compressing or decompressing the encryption key using a predetermined compression and decompression method, wherein the compressed encryption key is stored onto the non-volatile storage means and when the encryption key is used, the compressed encryption key is read from the non-volatile storage means as taught by Ronning '647.

The motivation for doing so would have been in order to prevent unauthorized copying of the software program or other digital information ("*...in order to prevent unauthorized copying of the software program or other digital information.*" Ronning '647 at column 2, lines 20-23).

Therefore, it would have been obvious to combine Kurihara '716, Bright '329 and Lee '613 with Ronning '647 to obtain the invention as specified in claim 1.

**Regarding claim 7;** Ronning '647 discloses an encryption key compression and decompression means for compressing or decompressing the encryption key using a predetermined compression and decompression method, wherein the compressed encryption key is stored onto the non-volatile storage means and when the encryption key is used, the compressed encryption key is read from the non-volatile storage means ("*The system decrypts the sectors while reading them. The encryption/decryption of sector is explained with reference to FIGS. 16A and 16B. If the sectors of the application are compressed the system also decompresses the sectors while reading them.*" column 8, lines 21-25). See also ("*An image file 77 which is the desired size of a "virtual volume" created by a software or digital information*



*distribution system is allocated on a hard drive 75 or other non-volatile storage medium."*  
column 6, lines 14-18).

**Regarding claim 8;** Ronning '647 discloses an encryption key compression and decompression means for compressing or decompressing the encryption key using a predetermined compression and decompression method, wherein the compressed encryption key is stored onto the non-volatile storage means and when the encryption key is used, the compressed encryption key is read from the non-volatile storage means ("*The system decrypts the sectors while reading them. The encryption/decryption of sector is explained with reference to FIGS. 16A and 16B. If the sectors of the application are compressed the system also decompresses the sectors while reading them.*" column 8, lines 21-25). See also ("*An image file 77 which is the desired size of a "virtual volume" created by a software or digital information distribution system is allocated on a hard drive 75 or other non-volatile storage medium.*" column 6, lines 14-18).

**Regarding claim 9;** Ronning '647 discloses an where the encryption key compression and decompression means applies an image compression and decompression unit for compressing or decompressing the image data ("*The system decrypts the sectors while reading them. The encryption/decryption of sector is explained with reference to FIGS. 16A and 16B. If the sectors of the application are compressed the system also decompresses the sectors while reading them.*" column 8, lines 21-25).

**Regarding claim 10;** Ronning '647 discloses an where the encryption key compression and decompression means applies an image compression and decompression unit for

compressing or decompressing the image data (*"The system decrypts the sectors while reading them. The encryption/decryption of sector is explained with reference to FIGS. 16A and 16B. If the sectors of the application are compressed the system also decompresses the sectors while reading them."* column 8, lines 21-25).

**Regarding claim 11;** Ronning '647 discloses an where the encryption key compression and decompression means applies an image compression and decompression unit for compressing or decompressing the image data (*"The system decrypts the sectors while reading them. The encryption/decryption of sector is explained with reference to FIGS. 16A and 16B. If the sectors of the application are compressed the system also decompresses the sectors while reading them."* column 8, lines 21-25).

8. **Claims 12, 13, 18 & 19** are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsuzaki '476 in combination with Ronning '647 as applied to claim 1 above, and further in view of Ote '506.

**Regarding claim 12;** Matsuzaki '476 discloses an image forming apparatus for forming an image based on input image data, the image forming apparatus comprising: input means for capturing a key value of an encryption key input by a user during the setting of the encryption key (*"In FIG. 3 step (11), the E function 67 uses data transfer key K stored in data transfer key K storage unit 70 to encrypt digital copyrighted material inputted through external I/F unit 61 and switch 65. The result Cj is outputted to second device 52 through switch 68 and external I/F unit 61."* column 15, lines 3-7); key value determining means for determining whether key values input by the user by a predetermined number of times match each other (*"First device 11*

*compares the decryption result RRI with the random number R1 temporarily stored inside first device 11. If they match, first device 11 considers second device 12 to be in possession of the same authentication key S, and confirms the entity in communication as a legitimate device. However if they do not match, then it judges the entity in communication an unauthorized device and terminates the process.*" column 2, lines 49-56).

Matsuzaki '476 does not expressly disclose a non-volatile storage means for storing the key value input as an encryption key if the key value determining means determines that the key values match each other or encryption and decryption means for encrypting the image data using an encryption key prior to the storage of the input image data onto image storage means, and for decrypting the encrypted image data subsequent to the reading of the encrypted image data from the image storage means.

Ronning '647 discloses a non-volatile storage means for storing the key value input as an encryption key if the key value determining means determines that the key values match each other (*"The system then determines if the loaded image matches the database image (196) for security purposes. If the image does not match, the database data is rectified to that of the image (198) and the virtual volume is closed and unmounted (194) in order to maintain the application in a locked state."* column 9, lines 5-9). See also (*"An image file 77 which is the desired size of a "virtual volume" created by a software or digital information distribution system is allocated on a hard drive 75 or other non-volatile storage medium."* column 6, lines 14-18); and encryption and decryption means for encrypting the image data using an encryption key prior to the storage of the input image data onto image storage means, and for decrypting the encrypted image data subsequent to the reading of the encrypted image data from the image storage means (*"The*

*system decrypts the sectors while reading them. The encryption/decryption of sector is explained with reference to FIGS. 16A and 16B. If the sectors of the application are compressed the system also decompresses the sectors while reading them.*" column 8, lines 21-25).

Matsuzaki '476 and Ronning '647 are combinable because they are from same field of endeavor of an image forming apparatus ("*The system typically uses an image driver 56...*" Ronning '647 at column 5, lines 19-20).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the image forming apparatus as taught by Matsuzaki '476 by adding a non-volatile storage means for storing the key value input as an encryption key if the key value determining means determines that the key values match each other or encryption and decryption means for encrypting the image data using an encryption key prior to the storage of the input image data onto image storage means, and for decrypting the encrypted image data subsequent to the reading of the encrypted image data from the image storage means as taught by Ronning '647.

The motivation for doing so would have been in order to prevent unauthorized copying of the software program or other digital information ("*...in order to prevent unauthorized copying of the software program or other digital information.*" Ronning '647 at column 2, lines 20-23).

Therefore, it would have been obvious to combine Matsuzaki '476 with Ronning '647 to obtain the invention as specified in claim 12.

Matsuzaki '476 with Ronning '647 does not expressly disclose displaying an image on a screen so as to prompt a user to input a key a plurality of times when power is on.

Ote '506 discloses displaying an image on a screen so as to prompt a user to input a key a plurality of times when power is on (*"Upon starting the file encryption/decryption means 1000 to conduct decryption, the file encryption/decryption means 1000 conducts authentication processing by using the password 1070 with respect to a user input password, then refers to the unencrypted file /encrypted file association table 1060, and displays a list of encrypted files 1090 stored in the encrypted file area 1080 in the form of unencrypted file names. In this state, the encryption folder 1040 is open. The user can select unencrypted files 1090 stored in the encrypted file area 1080 out of the list displayed in the form of unencrypted file names."* column 5, lines 5-15).

Matsuzaki '476 and Ronning '647 are combinable with Ote '506 because they are from same field of endeavor of an image forming apparatus (*"The user interface in an embodiment in which the present invention is applied to the operating system "MS-Windows" will now be described by using diagrams showing concrete images of the screen."* Ote '506 at column 13, lines 38-41).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the image forming apparatus as taught by the combination of Matsuzaki '476 and Ronning '647 by adding displaying an image on a screen so as to prompt a user to input a key a plurality of times when power is on as taught by Ote '506.

The motivation for doing so would have been to make it possible to encrypt files by effecting a simple manipulation (*"...and which makes it possible to encrypt files by effecting a simple manipulation..."* Ote '506 at column 2, lines 3-4).

Therefore, it would have been obvious to combine Matsuzaki '476 and Ronning '647 with Ote '506 to obtain the invention as specified in claim 12.

**Regarding claim 13;** Matsuzaki '476 in combination with Ronning '647 does not expressly disclose display means for displaying the key value captured by the input means, and converting an input key value into a form having no specific meaning.

Ote '506 discloses display means for displaying the key value captured by the input means, and converting an input key value into a form having no specific meaning ("*...and displays a list of encrypted files 1090 stored in the encrypted file area 1080 in the form of unencrypted file name.*" column 6, lines 9-12).

Matsuzaki '476 and Ronning '647 are combinable with Ote '506 because they are from same field of endeavor of an image forming apparatus ("*The user interface in an embodiment in which the present invention is applied to the operating system "MS-Windows" will now be described by using diagrams showing concrete images of the screen.*" Ote '506 at column 13, lines 38-41).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the image forming apparatus as taught by the combination of Matsuzaki '476 and Ronning '647 by adding display means for displaying the key value captured by the input means, and converting an input key value into a form having no specific meaning as taught by Ote '506.

The motivation for doing so would have been to make it possible to encrypt files by effecting a simple manipulation (*"...and which makes it possible to encrypt files by effecting a simple manipulation..."* Ote '506 at column 2, lines 3-4).

Therefore, it would have been obvious to combine Matsuzaki '476 and Ronning '647 with Ote '506 to obtain the invention as specified in claim 12.

**Regarding claim 18;** Matsuzaki '476 discloses a method for inputting the setting of an encryption key for use in the encryption of image data, the encryption key being used to store input image data in image storage means, the method comprising the steps of: capturing key values of the encryption key input by a user (*"In FIG. 3 step (11), the E function 67 uses data transfer key K stored in data transfer key K storage unit 70 to encrypt digital copyrighted material inputted through external I/F unit 61 and switch 65. The result Cj is outputted to second device 52 through switch 68 and external I/F unit 61."* column 15, lines 3-7); determining whether the key values input by the user by a predetermined number of times match each other (*"First device 11 compares the decryption result RRI with the random number R1 temporarily stored inside first device 11. If they match, first device 11 considers second device 12 to be in possession of the same authentication key S, and confirms the entity in communication as a legitimate device. However if they do not match, then it judges the entity in communication an unauthorized device and terminates the process."* column 2, lines 49-56).

Matsuzaki '476 does not expressly disclose storing, in non-volatile storage means, the input key value as the encryption key when the key values match each other in the key value determining step.

Ronning '647 discloses storing, in non-volatile storage means, the input key value as the encryption key when the key values match each other in the key value determining step (*"The system then determines if the loaded image matches the database image (196) for security purposes. If the image does not match, the database data is rectified to that of the image (198) and the virtual volume is closed and unmounted (194) in order to maintain the application in a locked state."* column 9, lines 5-9). See also (*"An image file 77 which is the desired size of a "virtual volume" created by a software or digital information distribution system is allocated on a hard drive 75 or other non-volatile storage medium."* column 6, lines 14-18).

Matsuzaki '476 and Ronning '647 are combinable because they are from same field of endeavor of an image forming apparatus (*"The system typically uses an image driver 56..."* Ronning '647 at column 5, lines 19-20).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the image forming apparatus as taught by Matsuzaki '476 by adding storing, in non-volatile storage means, the input key value as the encryption key when the key values match each other in the key value determining step as taught by Ronning '647.

The motivation for doing so would have been in order to prevent unauthorized copying of the software program or other digital information (*"...in order to prevent unauthorized copying of the software program or other digital information."* Ronning '647 at column 2, lines 20-23).

Therefore, it would have been obvious to combine Matsuzaki '476 with Ronning '647 to obtain the invention as specified in claim 18.

Matsuzaki '476 and Ronning '647 does not expressly disclose displaying an image on a screen so as to prompt a user to input a key a plurality of times when power is on.



Ote '506 discloses displaying an image on a screen so as to prompt a user to input a key a plurality of times when power is on (*"Upon starting the file encryption/decryption means 1000 to conduct decryption, the file encryption/decryption means 1000 conducts authentication processing by using the password 1070 with respect to a user input password, then refers to the unencrypted file /encrypted file association table 1060, and displays a list of encrypted files 1090 stored in the encrypted file area 1080 in the form of unencrypted file names. In this state, the encryption folder 1040 is open. The user can select unencrypted files 1090 stored in the encrypted file area 1080 out of the list displayed in the form of unencrypted file names."* column 5, lines 5-15).

Matsuzaki '476 and Ronning '647 are combinable with Ote '506 because they are from same field of endeavor of an image forming apparatus (*"The user interface in an embodiment in which the present invention is applied to the operating system "MS-Windows" will now be described by using diagrams showing concrete images of the screen."* Ote '506 at column 13, lines 38-41).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the image forming apparatus as taught by the combination of Matsuzaki '476 and Ronning '647 by adding displaying an image on a screen so as to prompt a user to input a key a plurality of times when power is on as taught by Ote '506.

The motivation for doing so would have been to make it possible to encrypt files by effecting a simple manipulation (*"...and which makes it possible to encrypt files by effecting a simple manipulation..."* Ote '506 at column 2, lines 3-4).

Therefore, it would have been obvious to combine Matsuzaki '476 and Ronning '647 with Ote '506 to obtain the invention as specified in claim 18.

**Regarding claim 19;** Matsuzaki '476 in combination with Ronning '647 does not expressly disclose wherein the displaying step displays the key value captured in the capturing step, and converts an already input key value into a form having no specific meaning.

Ote '506 discloses wherein the displaying step displays the key value captured in the capturing step, and converts an already input key value into a form having no specific meaning ("*...and displays a list of encrypted files 1090 stored in the encrypted file area 1080 in the form of unencrypted file name.*" column 6, lines 9-12).

Matsuzaki '476 and Ronning '647 are combinable with Ote '506 because they are from same field of endeavor of an image forming apparatus ("*The user interface in an embodiment in which the present invention is applied to the operating system "MS-Windows" will now be described by using diagrams showing concrete images of the screen.*" Ote '506 at column 13, lines 38-41).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the image forming apparatus as taught by the combination of Matsuzaki '476 and Ronning '647 by adding a wherein the displaying step displays the key value captured in the capturing step, and converts an already input key value into a form having no specific meaning as taught by Ote '506.

The motivation for doing so would have been to make it possible to encrypt files by effecting a simple manipulation (“...and which makes it possible to encrypt files by effecting a simple manipulation...” Ote ‘506 at column 2, lines 3-4).

Therefore, it would have been obvious to combine Matsuzaki ‘476 and Ronning ‘647 with Ote ‘506 to obtain the invention as specified in claim 18.

9. **Claim 14** is rejected under 35 U.S.C. 103(a) as being unpatentable over Matsuzaki ‘476, Ronning ‘647 and Ote ‘506 as applied to claim 12 above, and further in view of Kobayashi et al. Kobayashi ‘094.

**Regarding claim 14;** Matsuzaki ‘476, Ronning ‘647 and Ote ‘506 does not expressly disclose where the display means divides the key value of M digits on an N digits by N digits basis (M being greater than N), and converts a part of the key value of the N digits into a form having no specific meaning as soon as the inputting of the key value of the part of the N digits is completed.

Kobayashi ‘094 discloses where the display means divides the key value of M digits on an N digits by N digits basis (M being greater than N), and converts a part of the key value of the N digits into a form having no specific meaning as soon as the inputting of the key value of the part of the N digits is completed (“The data server 10 divides text data into plural parts in accordance with image memory sizes, wherein, memory overflow can be prevented by transmitting the succeeding part when printing for one preceding part is completed, or when it is confirmed, even in the course of printing, that sufficient unoccupied capacity is secured for image memory, which is preferable.” column 18, lines 41-47).

Matsuzaki '476, Ronning '647 and Ote '506 are combinable with Kobayashi '094 because they are from same field of endeavor of an image forming apparatus ("*The present invention relates to a printing apparatus which conducts printing based on data expressing images...*" Kobayashi '094 at column 1, lines 7-8).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the image forming apparatus as taught by Matsuzaki '476, Ronning '647 and Ote '506 by adding where the display means divides the key value of M digits on an N digits by N digits basis (M being greater than N), and converts a part of the key value of the N digits into a form having no specific meaning as soon as the inputting of the key value of the part of the N digits is completed as taught by Kobayashi '094.

The motivation for doing so would have been to prevent printing failure and delay ("*... to provide a print system which prevents that printing failure and delay...*" Kobayashi '094 at column 2, lines 25-27).

Therefore, it would have been obvious to combine Matsuzaki '476, Ronning '647 and Ote '506 with Kobayashi '094 to obtain the invention as specified in claim 12.

10. **Claims 15 & 16** are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsuzaki '476, Ronning '647 and Ote '506 as applied to claim 12 above, and further in view of Ashizaki '500.

**Regarding claim 15;** Matsuzaki '476, Ronning '647 and Ote '506 does not expressly disclose where the inputting and displaying of the key value is performed in one of a decimal format and a hexadecimal format.

Ashizaki '500 discloses where the inputting and displaying of the key value is performed in one of a decimal format and a hexadecimal format (*"As shown in FIGS. 9 to 12, the print data specifying information is identified by a hexadecimal value of the name of an image format."* column 15, lines 4-6).

Matsuzaki '476, Ronning '647 and Ote '506 are combinable with Ashizaki '500 because they are from same field of endeavor of an image forming apparatus (*"The present invention relates to a... printing apparatus..."* Ashizaki '500 at column 1, lines 12-13).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the image forming apparatus as taught by Matsuzaki '476, Ronning '647 and Ote '506 by adding where the inputting and displaying of the key value is performed in one of a decimal format and a hexadecimal format as taught by Ashizaki '500.

The motivation for doing so would have been in order to make a printing work by the use of the print data supplied from the printing control unit via the second input/output means (*"...for making a printing work by the use of the print data supplied from the printing control unit via the second input/output means."* Ashizaki '500 at column 5, line 1-2).

Therefore, it would have been obvious to combine Matsuzaki '476, Ronning '647 and Ote '506 with Ashizaki '500 to obtain the invention as specified in claim 12.

**Regarding claim 16;** Matsuzaki '476, Ronning '647 and Ote '506 does not expressly disclose where the inputting and displaying of the key value is performed in one of a decimal format and a hexadecimal format.

Ashizaki '500 discloses where the inputting and displaying of the key value is performed in one of a decimal format and a hexadecimal format (*"As shown in FIGS. 9 to 12, the print data specifying information is identified by a hexadecimal value of the name of an image format."* column 15, lines 4-6).

Matsuzaki '476, Ronning '647 and Ote '506 are combinable with Ashizaki '500 because they are from same field of endeavor of an image forming apparatus (*"The present invention relates to a... printing apparatus..."* Ashizaki '500 at column 1, lines 12-13).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the image forming apparatus as taught by Matsuzaki '476, Ronning '647 and Ote '506 by adding where the inputting and displaying of the key value is performed in one of a decimal format and a hexadecimal format as taught by Ashizaki '500.

The motivation for doing so would have been in order to make a printing work by the use of the print data supplied from the printing control unit via the second input/output means (*"...for making a printing work by the use of the print data supplied from the printing control unit via the second input/output means."* Ashizaki '500 at column 5, lines 1-2).

Therefore, it would have been obvious to combine Matsuzaki '476, Ronning '647 and Ote '506 with Ashizaki '500 to obtain the invention as specified in claim 12.

11. **Claim 17** is rejected under 35 U.S.C. 103(a) as being unpatentable over Matsuzaki '476, Ronning '647, Ote '506 and Kobayashi '094 as applied to claim 12 above, and further in view of Ashizaki '500.

**Regarding claim 17;** Matsuzaki '476, Ronning '647, Ote '506 and Kobayashi '094 does not expressly disclose where the inputting and displaying of the key value is performed in one of a decimal format and a hexadecimal format.

Ashizaki '500 discloses where the inputting and displaying of the key value is performed in one of a decimal format and a hexadecimal format (*"As shown in FIGS. 9 to 12, the print data specifying information is identified by a hexadecimal value of the name of an image format."* column 15, lines 4-6).

Matsuzaki '476, Ronning '647, Ote '506 and Kobayashi '094 are combinable with Ashizaki '500 because they are from same field of endeavor of an image forming apparatus (*"The present invention relates to a... printing apparatus..."* Ashizaki '500 at column 1, lines 12-13).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the image forming apparatus as taught by Matsuzaki '476, Ronning '647, Ote '506 and Kobayashi '094 by adding where the inputting and displaying of the key value is performed in one of a decimal format and a hexadecimal format as taught by Ashizaki '500.

The motivation for doing so would have been in order to make a printing work by the use of the print data supplied from the printing control unit via the second input/output means (*"...for making a printing work by the use of the print data supplied from the printing control unit via the second input/output means."* Ashizaki '500 at column 5, lines 1-2).

Therefore, it would have been obvious to combine Matsuzaki '476, Ronning '647, Ote '506 and Kobayashi '094 with Ashizaki '500 to obtain the invention as specified in claim 12.

**Conclusion**

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Marcus T. Riley whose telephone number is 571-270-1581. The examiner can normally be reached on Monday - Friday, 7:30-5:00, est.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Twyler Lamb can be reached on 571-272-7406. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.



Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Marcus T. Riley  
Assistant Examiner  
Art Unit 2625

/Marcus T Riley/  
Examiner, Art Unit 2625

/Twyler L. Haskins/  
Supervisory Patent Examiner, Art Unit 2625